UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/990,001	11/21/2001	Futoshi Hachimura	B422-176	6301

26272 7590 06/22/2007
COWAN LIEBOWITZ & LATMAN P.C.
JOHN J TORRENTE
1133 AVE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/990,001	**Applicant(s)** HACHIMURA, FUTOSHI
	Examiner Longbit Chai	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 May 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,8-14,16-19 and 21-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,8-14,16-19 and 21-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 November 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1, 3 – 6, 8 – 14, 16 – 19 and 21 – 30.

Response to Arguments

2. Applicant's arguments and amendments filed on 5/30/2007 have been fully considered and are persuasive.

3. Applicant amends each of the independent claims by adding the claim limitation "the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is transmitted". First, Examiner notes: "when the decrypted E-mail message is transmitted" is broadly interpreted as "when the decrypted E-mail message is transmitted to the client (or the recipient)". Besides, Anderson teaches (a) the sender can indicate whether the message should be transmitted in an encrypted manner. If the message is to be encrypted, the Message Sender retrieves the server system's public encryption key and uses the key to encrypt the message before sending the message to the MDS system (Anderson: Para [0023]) and (b) the Message Distributor (i.e. MDS) then determines for each recipient (e.g., from the message sending information), after decrypting the message, whether the message indicator is to be encrypted when the indicator is sent to that recipient. **If so**, the Message Distributor retrieves the public key for the recipient's computer system and uses the key to encrypt a copy of the message indicator (i.e. re-encrypted by a public key of the client) (Anderson: Para [0025]). Therefore, Examiner notes Anderson does teach including an alternative of receiving a message at the client (i.e. **Else-condition**) that the decrypted E-mail message, at the MDS, being not re-encrypted using a public key when the decrypted E-mail message is transmitted to the recipient and as such Applicant's arguments are respectfully traversed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3, 6, 8 – 14, 16, 19 and 21 – 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wright et al. (U.S. Patent 2002/0016910), in view of Saliba et al. (Patent Publication Number: 2001/0037315), and in view of Anderson (U.S. Patent 2002/0052923).

As per claim 1, 13, 14, 26 – 30, Wright teaches a communication system having a server for providing a Web E-mail service to a Web browser (Wright: Para [0054] Line 12 – 16 and Para [0064] Line 1 – 7) of a client, wherein said server comprises:

management means for managing a key for decrypting an encrypted E-mail message addressed to a user's mail address (Wright: Para [0058] and Para [0064] Line 1 – 7), the E-mail message being encrypted by public key corresponding to the user's mail address (Wright: Para [0074] Line 13 – 15), wherein the secret key corresponding to the user's mail address for decrypting the encrypted E-mail message is not managed by the Web browser of the client (Wright: Para [0058]: the security key can be managed by the server; instead of the client).

Wright does not disclose expressly web encryption communication means for establishing a Web encryption communication with the client, and communicating with the client by the Web encryption communication established by said web encryption communication means.

Saliba teaches web encryption communication means for establishing a Web encryption communication with the client, and communicating with the client by the Web encryption communication established by said web encryption communication means (Saliba: Para [0120]: SSL provides the lower level data encryption communication).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Saliba within the system of Wright because (a) Wright teaches providing e-Mail access through web URL (Wright: Para [0064], [0054] and [0056]) , and (b) Saliba teaches providing e-Mail distribution by protecting the URL via SSL encryption to enhance the security (Saliba: Para [0120]).

authentication means for executing authentication of a use of allowance of the key managed by said management means to the client (Wright: Para [0020] Line 1 – 10). However, Wright does not disclose expressly the Web browser of the client requests to decrypt the encrypted E-mail message.

Anderson teaches the Web browser of the client requests to decrypt the encrypted E-mail message (Anderson : Para [0006] Line 9 – 12, Para [0007] and Para [0027]: the server can perform message decryption if necessary).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Anderson within the system of Wright because (a) Wright teaches providing an improvement of efficiency and competency of electronic message delivery system (Wright: Para [0008]), and (b) Anderson teaches providing a more flexible as well as more beneficial mechanism of electronic message delivery system with user's option to handle the electronic messages by simply sending user's request and instructions to the message server system (Anderson : Para [0006] Line 9 – 12 and Para [0007]).

decrypting means for making a decrypted message by decrypting said encrypted E-mail message using the secret key managed by said management means is authenticated by said authentication means (Anderson: Figure 5 Element 515 / Element 550, Para [0006] Line 9 – 12, Para [0027] and Para [0038] – [0039])., the secret key corresponding to the user's mail address, in the case where the allowance of the secret key managed by said management means is authenticated by said authentication means (Wright: Para [0058] and Para [0060]: the security key can be managed by the server; or, instead may reside on the client – i.e. the secret key corresponding to the user's mail address and the client may need to be authenticated by correct key-phrase); and

transmission control means for controlling to transmit the decrypted E-mail message decrypted by said decrypted means to the client through the Web encryption communication established by said web encryption communication means (Wright: Para [0064] Line 1 – 7, Para [0020] Line 1 – 10 and Para [0058] Last sentence: (a) to deliver the E-mail across the network such as internet URL (HTTP) over the network to deliver the message to the client and the decryption of the message / document can be done at the 3rd party, such as a server as an alternative) and (b) (Anderson: see for example, Para [0019] Line 6 – 10: to deliver the E-mail across the network such as internet URL (HTTP) through various nodes and links until it reaches the recipient users) and (c) (Saliba: Para [0120]),

the decrypted E-mail message being not re-encrypted by a public key when the decrypted E-mail message is transmitted (Anderson: Para [0023] and [0025]: (a) the sender can indicate whether the message should be transmitted in an encrypted manner. If the message is to be encrypted, the Message Sender retrieves the server system's public encryption key and uses the key to encrypt the message before sending the message to the MDS system (Anderson: Para [0023]) and (b) the Message Distributor (i.e. MDS) then determines for each recipient (e.g., from the message sending information), after decrypting the message, whether the message indicator is to be encrypted when the indicator is sent to that recipient. **If so**, the Message Distributor retrieves the public key for the recipient's computer system and uses the key to encrypt a copy of the message indicator (i.e. re-encrypted by a public key of the client). Therefore, Examiner notes Anderson does teach including an alternative of receiving a message at the client (i.e. **Else-condition**) that the decrypted E-mail message, at the MDS, being not re-encrypted using a public key when the decrypted E-mail message is transmitted to the recipient (Anderson: Para [0025])).

As per claim 3 and 16, Wright as modified teaches said authentication means provides said client with a window data to authenticate the use allowance of the managed key (Wright: Para [0058] and Para [0054]: web-based application must be window-oriented).

As per claim 4 and 17, Wright as modified teaches said authentication means authenticates the use allowance using a passphrase inputted from said client (Wright: Para [0020]).

As per claim 5 and 18, Wright as modified teaches said authentication means authenticates the use allowance based on a biometrics information of a user inputted from said client (Wright: Para [0015]).

As per claim 6 and 19, Wright as modified teaches said web encryption communication means establishes the Web encryption communication with the client by using SSL (Wright:

Para [0056]) & (Saliba: Para [0120]: SSL provides the lower level data encryption communication).

As per claim 8 and 21, Wright as modified teaches said authentication means authenticates the use allowance of the managed key during a session of the Web encryption communication continuously established between said client and a server (Wright: Para [0056]) & (Saliba: Para [0120]: SSL provides the lower level data encryption communication).

As per claim 9 and 22, Wright as modified teaches said authentication means stops said authenticated use allowance, in the case where at least either the case where said encryption communication is ended with an error or the case where said encryption communication has passed a fixed time is satisfied (Wright: Para [0056] – This is part of the typical features for encrypted web communication HTTP / SSL layer that is also described in the specification of the instant application (SPEC: Page 14 Line 6 – 14)).

As per claim 10 and 23, Wright as modified teaches said server further comprises signature means for executing a digital signature to an E-mail required for the digital signature by said client (Wright: Para [0015]).

As per claim 11 and 24, Wright as modified teaches managing whether said key is under multiple use, an said management means comprises stop means for stopping the use allowance of said session under multiple use in the case where said session is judged to be under multiple use (Wright: Para [0007]: the private key is unique to a specific user).

As per claim 12 and 25, Wright as modified teaches the key for decrypting said encrypted E-mail is a secret key in a code of a public key cryptosystem (Wright: Para [0020]).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100